Protection of Records and Data Authentication based on Secret Shares and Watermarking

Protection of Records and Data Authentication based on Secret Shares and Watermarking

Zulfiqar Ali[1], Muhammad Imran[2], Sally McClean[3], Naveed Khan[1], Muhammad Shoaib[2]

[1]School of Computing, Ulster University, Newtownabbey BT37 0QB, UK.
[2]College of Compter and Information Sciences, King Saud university, Riyadh 11543, Saudi Arabia.
[3]School of Computing, Ulster University, Coleraine BT52 1SA, UK.

Email: z.ali@ulster.ac.uk

ABSTRACT

The rapid growth in communication technology facilitates the health industry in many aspects from transmission of sensor's data to real-time diagnosis using cloud-based frameworks. However, the secure transmission of data and its authenticity become a challenging task, especially, for health-related applications. The medical information must be accessible to only the relevant healthcare staff to avoid any unfortunate circumstances for the patient as well as for the healthcare providers. Therefore, a method to protect the identity of a patient and authentication of transmitted data is proposed in this study. The proposed method provides dual protection. First, it encrypts the identity using Shamir's secret sharing scheme without the increase in dimension of the original identity. Second, the identity is watermarked using zero-watermarking to avoid any distortion into the host signal. The experimental results show that the proposed method encrypts, embeds and extracts identities reliably. Moreover, in case of malicious attack, the method distorts the embedded identity which provides a clear indication of fabrication. An automatic disorder detection system using Mel-frequency cepstral coefficients and Gaussian mixture model is also implemented which concludes that malicious attacks greatly impact on the accurate diagnosis of disorders.

1. INTRODUCTION

Healthcare is a basic need of every human being. The increasing world population is one of the major problems that confronts the traditional methods of providing health facilities, in which patients schedule appointments, visit hospitals, and wait for hours to see specialists. The limitations of the old-style methods of providing healthcare can be avoided through automatic diagnosis systems [1]. Several automatic health monitoring systems are designed and developed in [2, 3], which can be used in smart homes and cities. Such systems can process the data collected through the Internet of Things (IoT) and may provide the results to patients without any delay and loss of time and money. Although IoT and communications technology allow the centralized computing and storage of data, data privacy is a prime concern as well [4]. The objective of this study is to develop and implement a privacy protection method with a dual security feature using encryption and watermarking.

Visual cryptography can be used to encrypt a patient's identity by generating secret shares [5]. An approach for visual cryptography to produce two secret shares from an identity (black-and-white) is implemented in [6, 7]. The dimension of each generated share is 40 × 252, whereas that of each original identity is 20 × 126. The creation of secret shares of double dimension compared with the original identity needs substantially large space to be inserted in a signal. Both secret shares need a space of 20,160 bits, which are 800% more than the space needed by the original identity (i.e., 2,520 bits). This situation becomes considerably adverse if the identity is a grayscale image. Each grayscale image contains 8 bit-planes and a secret share will be generated for each bit-plane. In [8], visual cryptography is used to encrypt mammograms to avoid exposing the medical condition of a patient. The mammograms are the grayscale images with the 8-bit pixel values that range from 0 to 255. Two encrypted secret shares are generated for each bit plane. Consequently, 16 encrypted shares are produced for 1 mammogram. In [9], visual cryptography is implemented to encrypt the biometric data to avoid breach. Given that biometric images are grayscale images, 16 secret shares were generated in this case for each image. Hence, numerous bits are required to accommodate all shares during watermarking, although such a large capacity is nearly inapplicable in certain situations. Therefore, a suitable approach for visual cryptography should be used to prevent the dimension of the secret shares from surpassing that of the original identity.

In addition, the generated secret shares can be embedded into a signal through watermarking for dual protection of patient's identity. One of the common approaches in watermarking is the insertion of patients' information in the region of non-interest (RONI). RONI represents the areas that are unaffected by lesion. The insertion of the watermark in these areas does not affect the diagnosis of a disorder. However, an erroneously detected RONI in a signal may lead to false diagnosis [10, 11]. Therefore, the approach-based RONI may be unsuitable for privacy protection in medical signals. Similarly, conventional watermarking distorts the

Figure 1: Causes of vocal fold disorders.

signal after the insertion of a patient's identity, which is not good for medical data. In [12], a privacy protected framework based on traditional watermarking is presented. The identity of a person is protected using discrete wavelet transformation (DWT) and singular value decomposition (SVD). Such approach may result in false diagnosis because of the distortion introduced by watermarking in a signal [13, 14]. In reversible watermark, the watermark is extracted before the diagnosis, which does not affect the diagnosis. However, the major drawback of this approach is that medical images become vulnerable after identity extraction [15, 16]. To avoid the limitation of such types of watermarking, various algorithms for zero-watermarking has been proposed in literature.

In [17, 18], zero-watermarking methods for images are described. An image contains several stable parts which are ideal for insertion of physical watermarks in case of traditional watermarking. For zero-watermarking, features from those part can be computed to embed watermarks. Unlike to images, speech signals are difficult to handle as they vary quickly over time. As a result, the properties of speech signals do not remain same. This might be the reason that a little work of zero-watermarking using speech signals is available in literature as compared to images.

Recently, a chaos-based method for zero-watermarking is presented in [19]. The method uses the logistic map to introduce the deterministic randomness which makes the method strong from authorized access to patient data. Moreover, to make the method robust against noise, low-frequency regions of speech signals are determining for watermarking. The robustness helps in extraction of patients' identities perfectly, but it does not provide any proof about originality of data. In other words, the method is unable to authenticate the data of a sender. In addition, the patient's identity is directly used for watermarking without any encryption. Similarly, in another study [20], an identity of a patient is directly used for protection of privacy in telemedicine. The method describes the insertion and extraction processes but does not provide the effect of these processes on diagnosis of vocal folds disorders [21-23].

The vocal folds reside on the top of the trachea (windpipe) and are made with small folds of muscles and tissues. Vocal folds open and close in regular intervals during phonation to produce a healthy voice [24]. The voice of a person can be considered as healthy if he/she can meet the personal and professional requirement of the voice in a daily life without facing any fatigue and vocal problems [25]. Vocal fold disorders, sometimes also referred as vocal fold lesions or vocal fold pathologies, appear due to different reasons. Generally, vocal misuse including yelling, excessive talking, screaming and crying cause irritating forces at the contact place of two vocal folds, as indicated by Fig. 1.

This study uses a suitable approach for visual cryptography to generate secret shares, such that the dimensions of all generated shares should not exceed the dimension of the original patient's identity. This way, the issue of capacity during the watermarking process can be avoided. Moreover, the zero-watermarking approach is used to watermark the generated shares. Zero-watermarking inserts the identity into a secret key instead of the signal. Hence, the signal remains in the original form and does not change its properties, which is vital for the accurate diagnosis of diseases. For a reliable insertion of patient's identity, the secret shares are inserted in unvoiced frames of signals. The speech signals of patients suffering from vocal fold disorders are considered to protect their respective identities [26]. The proposed zero-watermarking method has the following characteristics:

- Dual protection for privacy protection using visual encryption and zero-watermarking.
- Implementation of an appropriate approach for visual cryptography to avoid capacity issue.

- Insertion of secret shares at appropriate location decided by using computed features.
- Effect of malicious attack on disorder detection using voice features and machine learning algorithm.
- Integrity of patient's data for reliable detection of disorders.

The rest of the paper is organized as follows: Section 2 describes the vocal folds disorder database and all components of the proposed method. Section 3 elaborate the process for encryption and insertion of patient information and its evaluation. This section also explains the decryption and extraction process and its validation. Section 4 provides the information about automatic disorder detection system and determines the authenticity of data. The effect of malicious attack on accurate diagnosis is also discussed in this section. Section 5 gives comparison of the proposed method with the existing methods. Finally, Section 6 draws some conclusion and provides future directions.

2. MATERIAL AND METHOD

The proposed zero-watermarking method is validated for real world scenario by considering the medical data of patients affected by vocal folds disorders. The data is publicly available through PANTEX Medical.

2.1 Vocal Folds Disorder Database

Vocal fold disorders can be classified into different groups depending upon the causes of occurrence. A vocal fold disorders can appear due to abnormal growth of tissues on the vocal folds. These types of disorder are known as benign lesions [27, 28], and they are non-cancerous in nature. The vocal fold disorders may also appear due to nerve's injury which controls the vibration of vocal folds [29]. Paralysis is an example of such types of disorder. Another type of disorder is Keratosis which is considered as a precancerous lesion and occurs due to the presence of unusual cells on the vocal folds [30]. Moreover, adductor is a type of spasmodic dysphonia which appears due to neurological disorder [31].

Different types of vocal fold disorders including, benign lesions, nerves-related disorders, and precancerous disorders are considered in this study and taken from the Massachusetts Eye & Ear Infirmary (MEEI) vocal fold disorder database [32]. The MEEI database is recorded at two sampling frequencies, 25 kHz and 50 kHz. All samples are down-sampled to a unique frequency, i.e., 25 kHz, before zero-watermarking. The MEEI database has been used in many studies [33-35]. A subset of MEEI database containing 256 speech signals of running speech is used to evaluate the proposed method. In this subset, 53 normal and 173 patients have recorded rainbow passage. The text of the passage and distribution of the pathological signals among various vocal folds disorders is provided in [36]. The number of signals for adductor is 22, for nodules is 20, and for keratosis is 26, for polyp is 20, and for paralysis is 85.

2.2 Proposed Method for Privacy Protection

The proposed method for privacy protection has two major components. The first component is responsible for the generation of secret share using visual cryptography, while the second component is responsible for hiding the secret shares using zero-watermarking approach. The block diagram of the proposed method is shown in Figure. 2.

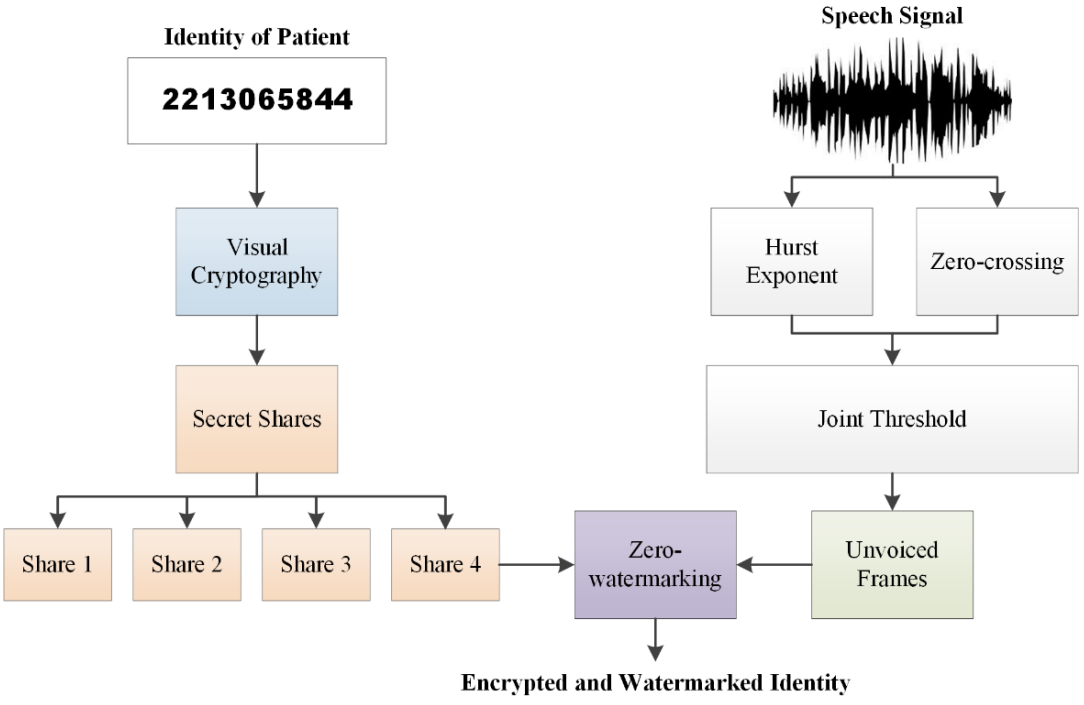


Figure 2: The block diagram of the proposed method for privacy protection

The first component generates secret shares using Shamir's secret sharing scheme [37]. Four shares are generated from the original identity and the dimension of each share is 10×90. The total dimension of all shares is equal to the dimension of the original identity.

The second component determines the unvoiced frames because they provided reliable locations to hide the generated shares. The unvoiced frames of the speech signals are determined by computing the Hurst exponent [38] and zero-crossing [39]. The Hurst exponent (E_H) is one of the reliable tools for fractal examination of time series and is computed using rescaled range (R/S) analysis in this study. The range of E_H for a frame always stays between 0 and 1. The value of E_H around 0.5 represents a random walk. The value between 0.5 and 1 describes the consistency such that if the waveform of a frame is in increasing trend then it will keep increasing, and similarly, if the waveform is decreasing then it will keep decreasing. The behavior of the waveform for E_H between 0 and 0.5 is anti-persistent, which describes that the increasing trend will start decreasing and vice versa. The other measure computes the zero-crossing (Z_C) of the waveform in a frame. Frames containing silence and unvoiced segments of speech have high-frequency of zero-crossing. However, unvoiced segments of speech have higher amplitude as compared to silence segments. In addition, voiced segments of speech have low zero-crossing and high amplitude. To identify the unvoiced frames of a speech signal, thresholds on both measures are applied based on conducted experiments. An unvoiced frame will satisfy both thresholds simultaneously to make sure that the frame is unvoiced.

After highlighting the unvoiced frames, the next step is calculation of features in each frame to watermark the generated secret shares. The features are calculated by applying Local Binary Pattern (LBP) operator on magnitude of each element of frames [40], and they are referred as Amp-LBP. The process of computing Amp-LBP is described in Figure 3. To compute Amp-LBP codes, the unvoiced frames are divided into windows of five elements, such that the center element represents the average amplitude and is denoted by *C*.

Thereafter, *C* is compared with its neighbors to generate 4-bit binary numbers within the range of 0000 to 1111. If C is greater or equal to the neighboring element then the element is replaced by a one, otherwise, the neighboring element is replaced by zero. In this way, 4-bit code for each window of a frame is calculated. The computed codes are further classified into two groups; uniform codes and non-uniform codes. Uniform codes refer to those which have less than two 0-to-1 or 1-to-0 transitions. For examples, the codes 0111, 0000, 1000, 1111 are uniform. Non-uniform codes bear more than one 0-to-1 or 1-to-0 transitions such as 0110, 1010, 1001 and 0101. In addition, equivalent decimal number is computed for the computed codes to determine the frequency of each code. During insertion and extraction of identity, uniform and non-uniform codes are used. Both insertion and extraction processes are highly sensitive to the Amp-LBP codes.

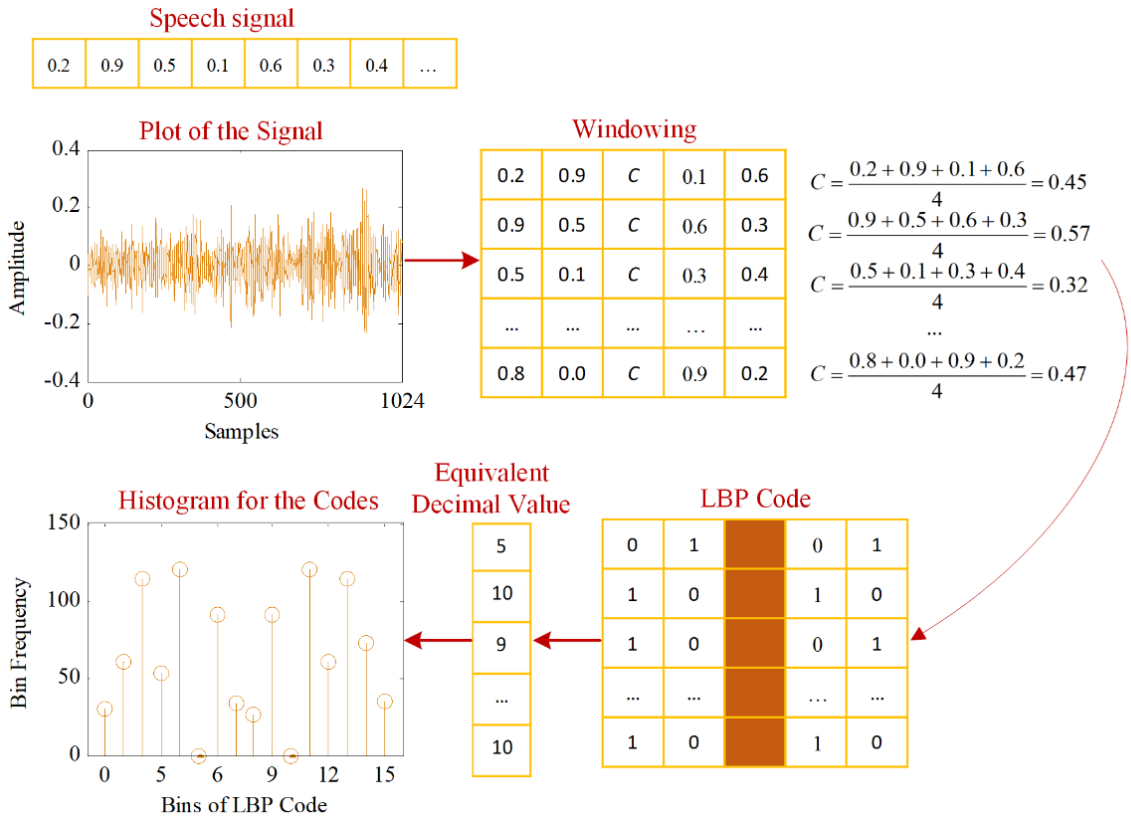


Figure 3: Step to calculate Amp-LBP code for an unvoiced frame.

3. PRIVACY PROTECTION

The major processes of the proposed method for protection of patient's information are: (1) encryption and zero-watermarking, and (2) decryption and recovery of identity. Both processes are explained and evaluated in this section by conducting number of experiments.

3.1 Encryption and Zero-Watermarking of Identity

The process for the protection of patient's identity using the proposed method is explained with the following steps. The block diagram of the process is given in Fig. 4.

1. Generate an image M for the identity of a patient with the dimension equivalent to $r_m \times c_m$.
2. Produce four secret shares S_1, S_2, S_3 and S_4 from the identity image M using Shamir's threshold scheme [37]. The dimension of each generated share is $r_s \times c_s$, where $r_s = r_m/2$ and $c_s = c_m/2$. The produced shares are shown in Fig. 5.
3. Divide the host speech signal G into short frames g_i such that the length of each frame can carry a secret share. The criteria for the length of a frame is given by Eq. 1.

$$LEN(g_i) > (r_s * c_s), \quad i = 1, 2, 3, ..., N \qquad (1)$$

where LEN represents the length of frame, '*' denotes the multiplication operation, and N stands for the total number of frames.

4. Identify unvoiced frames from g_i using criteria based on Hurst Exponent E_H and zero-crossing Z_C. The indices of unvoiced frames (u_k) are given by Eq. 2.

$$u_k = \{i | i \text{ is index of unvoiced frame and } k \leq N\} \qquad (2)$$

5. Randomly select four unvoiced frames, u_{k1}, u_{k2}, u_{k3} and u_{k4}, to accommodate the four secret shares and save the indices of the frames to use during the recovery process.
6. Now, to calculate the Amp-LBP codes for selected unvoiced frames, divide each frame into short windows. Then, generate intermediate keys T_j for each frame.
7. Intermediate keys T_j contain zero if the computed code is uniform in a window and hold a one if the code is non-uniform. The criteria to generate keys T_j is given by Eq. 3.

$$T_j = \begin{cases} 0 & \text{if } Amp\_LBP \text{ is Uniform} \\ 1 & \text{if } Amp\_LBP \text{ is Non} - \text{uniform} \end{cases} \qquad (3)$$

where j=1, 2, 3, and 4.

8. To enhance the security of the embedding process, the intermediate keys T_j are randomized by performing bitwise AND operation with normally distributed random sequences D_j of 0s and 1s. Consequently, the random secret keys R_j are obtained as given by Eq. 4.

$$R_j = D_j \,\&\, T_j, \text{where } j = 1,2,3,4. \qquad (4)$$

9. Finally, to embed the first secret share S_1 of the identity image M, perform exclusive-OR operation between the random secret key R_1 and the first secret share S_1 as given by Eq. 5. As a result, a watermark key w_1 is obtained.

$$w_1 = R_1 \oplus S_1 \qquad (5)$$

10. Repeat steps 6 to 9 for embedding of the remaining three secret shares S_2, S_3 and S_4. It will yield the watermarks keys w_2, w_3 and w_4, respectively, as mentioned in Eq. 6-8.

$$w_2 = R_2 \oplus S_2 \qquad (6)$$

$$w_3 = R_3 \oplus S_3 \qquad (7)$$

$$w_4 = R_4 \oplus S_4 \qquad (8)$$

The watermark keys w_1, w_2, w_3, w_4 with the indices of the unvoiced frames and random sequence D_1, D_2, D_3, D_4 need to be transmitted to the healthcare staff for accurate recovery of the patient's identity. The host signal G will also be transmitted to the healthcare staff for the diagnosis.

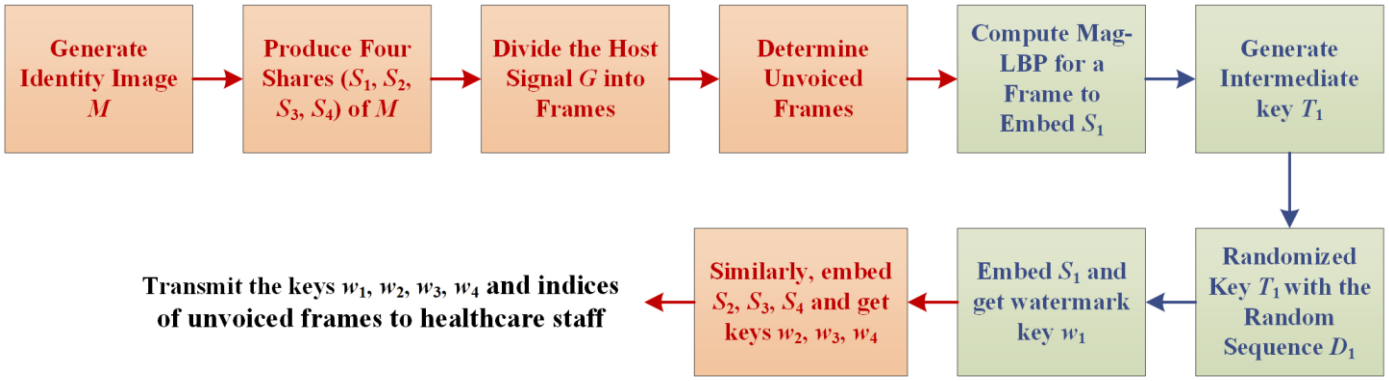


Figure 4: Steps for insertion of identity using visual cryptography and zero-watermarking.

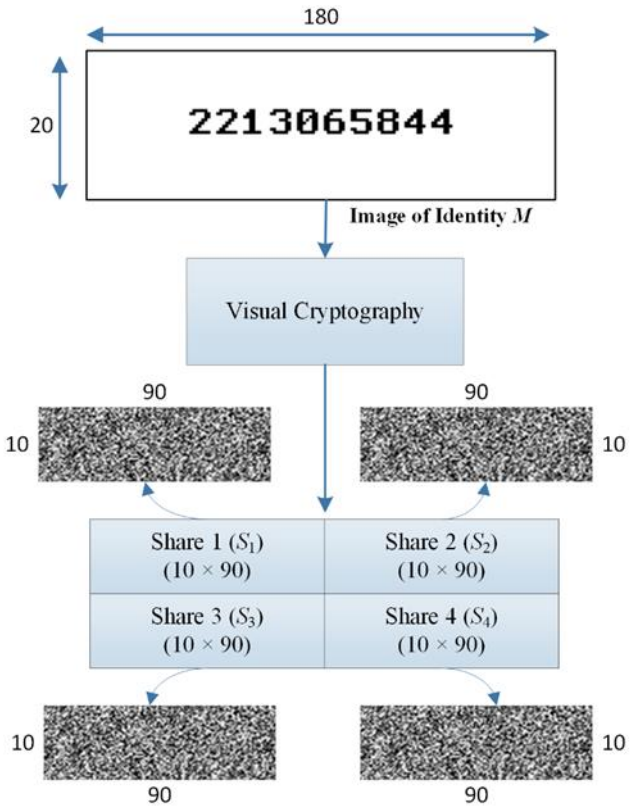


Figure 5: The four secret shares generated by visual cryptography.

3.2 Decryption and Recovery of Identity

After receiving the four watermark keys w_1, w_2, w_3, w_4 by the authorized healthcare staff, each staff member will recover a secret share using the following steps of the proposed method.

1. Divide the transmitted signal G' into frames of length LEN.
2. Compute the Amp-LBP code for the unvoiced frames whose indices u_{k1}, u_{k2}, u_{k3} and u_{k4} are provided to healthcare staff. Each staff member is responsible for the one of the unvoiced frames.
3. Generate intermediate key T_1' such that it contains zero if the computed Amp-LBP code is uniform. In case of non-uniform code, the key T_1' contains a one. This criterion is provided in Eq. 9. Similarly, compute other intermediate keys T_2', T_3' and T_4'.

$$T_1' = \begin{cases} 0 & \text{if } Amp\_LBP \text{ is uniform} \\ 1 & if \quad Amp\_LBP \text{ is non} - \text{uniform} \end{cases} \qquad (9)$$

4. Perform bitwise AND operation between the generated key T_1' and the transmitted random sequence D_1 to obtain the random secret key R_1', as given by Eq. 10.

$$R_j' = D_j \,\&\, T_j', \text{where } j = 1,2,3,4. \qquad (10)$$

5. Then, to recover the first secret share S_1', perform exclusive-OR operation between the obtained random secret key R_1' and the transmitted watermark key w_1 as given by Eq. 11.

$$S_1' = R_1' \oplus w_1 \qquad (11)$$

Similarly, other staff members recover the secret shares S_2', S_3' and S_4' as:

$$S_2' = R_2' \oplus w_2 \qquad (12)$$

$$S_3' = R_3' \oplus w_3 \qquad (13)$$

$$S_4' = R_4' \oplus w_4 \qquad (14)$$

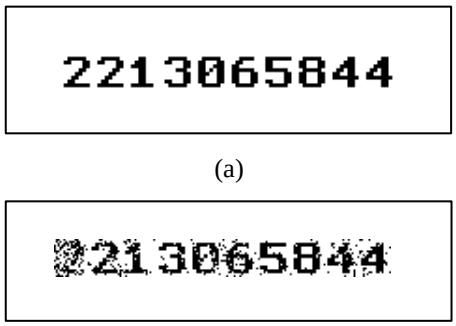
6. Finally, Shamir threshold scheme is applied on recovered secret shares S_1', S_2', S_3' and S_4' to extract the identity of the patient which is named as M'.

The next objective is to evaluate the processes of the proposed method to observe the reliability and accuracy.

3.3 Evaluation of Encryption and Watermarking Process

The protection of privacy depends on the quality of the encryption and insertion process, which consists of visual cryptography and zero-watermarking. The visual cryptography divides the generated identity image M into four equal encrypted secret shares S_1, S_2, S_3 and S_4 as shown in Fig. 5. The dimension of M is 20 × 180 and that are for each encrypted share is 10 × 90. As the number of pixels in each share is 900, therefore, the host audio signal G is divided into the frames of length 1024, i.e. LEN=1024, to accommodate pixels of a share.

The shares are watermarked in the unvoiced frames because the voiced frames cannot disguise the identity properly. For instance, the original identity image M is watermarked in the voiced frames and shown in Fig. 6. It can be observed that the identity is not disguised properly, which concludes that the voiced frames are unsuitable for watermarking of the identity. This is the reason that the shares are watermarked in the unvoiced frames which are determined by computing two measures, Hurst exponent E_H and zero-crossing Z_C. The unvoiced frames are determined by the criteria given in Eq. 15. An unvoiced and voiced frame of a speech signal are shown in Figure 7(a) and 7(b), respectively.

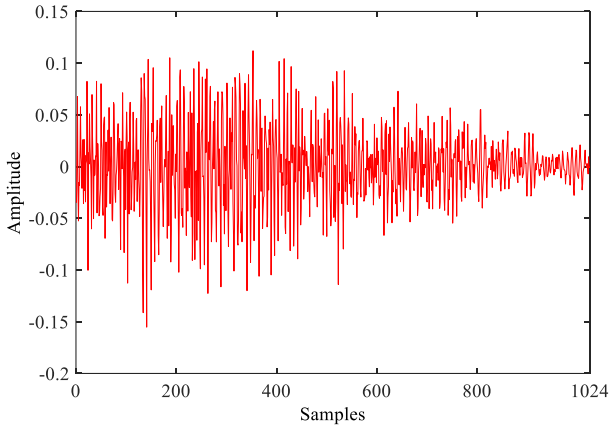


(a)

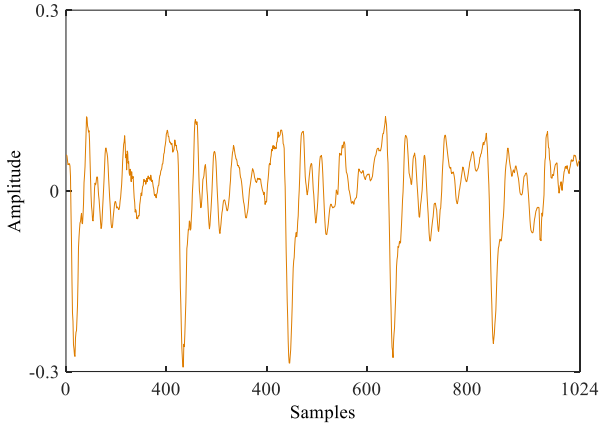
(b)

Figure 6: (a) Original identity M (b) M watermarked in voiced frames.

$$E_H < 0.5 \text{ and } Z_C > 350 \qquad (15)$$



(a)



(b)

Figure 7: (a) Unvoiced frame (b) Voiced frame.

The unvoiced frame contains significant randomness which makes it an ideal place for watermarking. On contrary, the voiced frame follows a regular pattern throughout the frame which is unable to disguise the identity properly.

One of the encrypted secret shares before and after watermarking by using an unvoiced frame having E_H = 0.2405 and Z_C= 536 are shown in Fig. 8. Apparently, it seems that both shares are same. In fact, they are significantly different from each other.

(a) (b)

Figure 8: (a) Encrypted secret share (b) Encrypted and watermarked secret share.

Two metrics, bit-error rate (ERT) and peak signal-to-noise ratio (PSNR) defined in Eq. 16 and 17, respectively, are used for the objective analysis of the shares shown in Fig. 8. The same metrics are used to observe the difference of all identities present in the vocal folds disorder database.

$$ERT = \frac{erroneous\ bits}{total\ bits} * 100 \qquad (16)$$

$$PSNR = 20\log_{10}\left(\frac{2^B - 1}{mse}\right) \qquad (17)$$

where *erroneous bits* represent the dissimilar bits at the corresponding locations of the shares. Moreover, *total bits* represent the number of pixels in a share, *B* denotes the number of bytes per pixels, i.e., 1 in our case, and *mse* stands for the mean squared error.

The computed ERT and PSNR for the encrypted and encrypted-watermarked shares are 55% and 8.29 dB, respectively. The higher value of ERT and lower value of PSNR signifies that the encrypted and encrypted-watermarked shares are entirely different from each other. Both metrics are computed for all samples of MEEI subset and depicted in Fig. 9 and 10. It can be observed from Fig. 8 that ERT is greater than 50% for all speech samples. Such high value of ERT shows that the watermarked shares are significantly different than the encrypted shares. Therefore, the encryption and watermarking process for protection of identity are secure and reliable. Similarly, the lower values of PSNR make the same conclusion because the values of PSNR towards zero occur only when the two images are significantly different from each other.

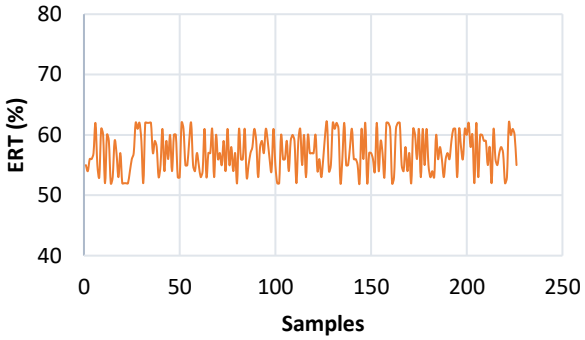


Figure 8: The average values of ERT for the encrypted and encrypted-watermarked shares for all speech samples.

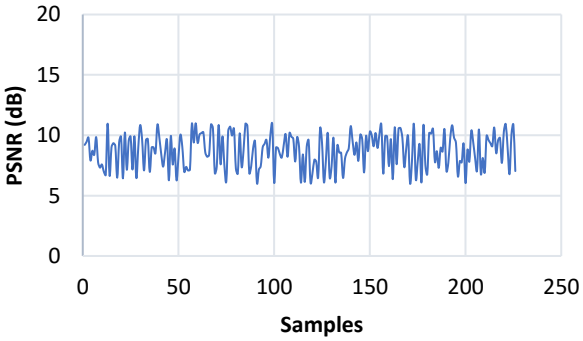
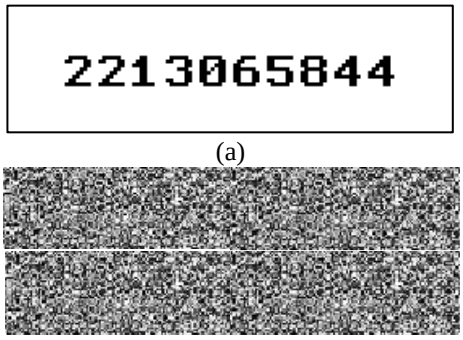


Figure 9: The average values of PSNR for the encrypted and encrypted-watermarked shares for all speech samples.

Moreover, many experiments are performed to watermark all speech signals of the MEEI database. To observe the quality of watermarking, the watermarked identities are objectively compared with the original identities using ERT and PSNR. Four shares are obtained for an identity as a result of

encryption and the dimension of each share is different than the dimension of original identity. Therefore, the original identity is not comparable with the watermarked shares. First, the shares are combined together as shown in Figure 10, and then, analysis is performed to observe the similarity to the original identity. After joining the shares, the obtained identity is referred as protected identity.



(a)

(b)

Figure 10: (a) Original identity (b) Protected identity.

After comparison, the obtained ERT is 85% which shows that the original and protected identities have a large number of different pixels at corresponding positions. The large value of ERT concludes that the quality of watermarking is good and there is no chance that the protected identity will reveal any information of a patient in case of unauthorized access. For these identities, the computed value of PSNR is 2%. It also strengthens the fact that the original and protected identities are entirely different, and the information of the patient is well protected. Similar analysis is performed for all signals of the database, and the computed performance measures are shown in Figure 11 and 12.

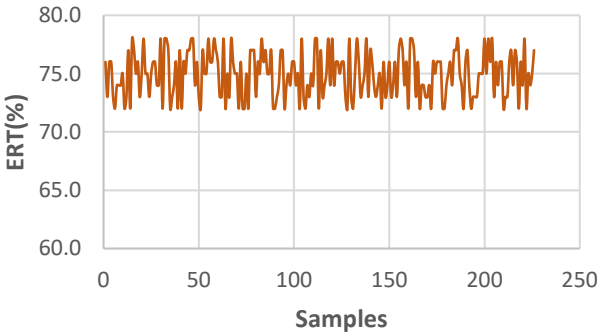


Figure 11: ERT for original and protected identities.

The computed average value of ERT is 74.9% with standard deviation of 1.9 for all signals of the MEEI database. It is also supported by Fig. 11 which shows that for all signals the ERT is around 75%. The higher values of ERT signify that the identities of all patients are embedded properly. Similarly, the lower values of PSNR concludes that all identities are disguised accurately. The average value of PSNR is 3.5 with the standard deviation of 0.3. Fig. 12 also shows that PSNR is around 3.5 for all signals.

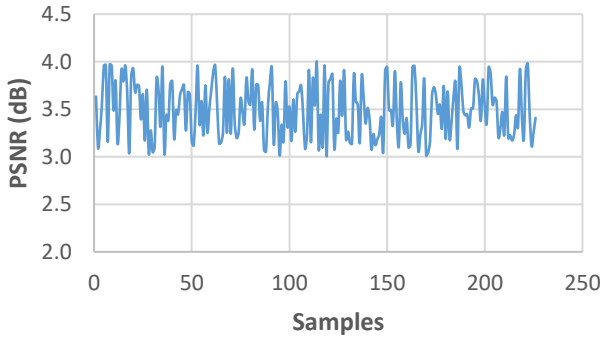


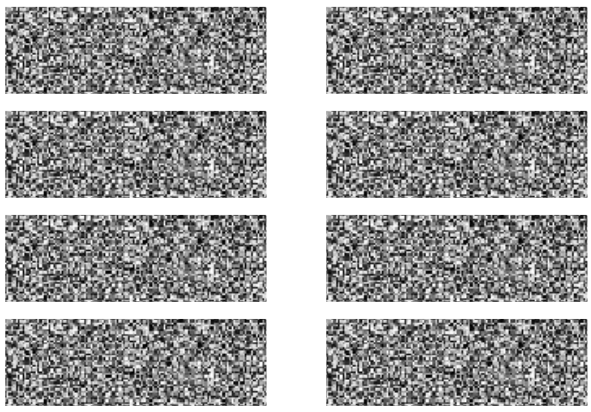
Figure 12: PSNR for original and protected identities.

In addition to the embedding of identity through encryption and watermarking, the accurate and reliable recovery of the patient identity is also very crucial for a protection method. Therefore, the recovery process of the proposed method is also needed to be evaluated.

3.4 Evaluation of Decryption and Recovery Process

The accurate recovery of patient's identity is very important to know the person whose speech signal is transmitted for the diagnosis. For successful recovery of the identity, each of the four staff members will extract the relevant secret share using the corresponding transmitted secret keys. Once all four secret shares are recovered, then they will be decrypted through visual cryptography to reveal the identity of the patient as shown in Fig. 13.

The objective analysis of the recovered secret shares (shown in Fig. 13) is performed by using the metrics given in Eq. 16 and 17. The ERT for the watermarked and recovered shares is 0%, which means that all secret shares are recovered perfectly. Moreover, the obtained values of the PSNR for all



(a) (b)

(c)

Figure 13: (a) Watermarked secret shares (b) recovered secret shares (c) decryption of recovered shares to obtain the identity.

shares are infinity because the value of *mse* in the denominator becomes zero when the share are similar. The *mse* equal to zero concludes that there is no error between the watermarked and recovered share. Therefore, it can be concluded that the recovery process of the proposed method is accurate and reliable.

Inaccurate diagnosis at a cost of protection cannot be acceptable. Therefore, the proposed method is evaluated to determine the authenticity of data so that accurate diagnosis of disorder should be made.

4 AUTHENTICITY OF MEDICAL DATA

Malicious attacks during the transmission of data change the properties of a signal. To do the objective analysis of change in properties, an automatic disorder detection system is implemented using Mel-frequency Cepstral Coefficients (MFCC) and Gaussian Mixture Model (GMM).

MFCC features mimic the behavior of the human auditory perception and has been widely used in many speech-related applications [41, 42]. The first step in calculation of MFCC features is blocking of the speech signals into short frames. Then, Fourier Transformation (FT) is applied to transform each frame from time to frequency domain and it also provides the contribution of each frequency component in a frame. The output of FT is referred as a spectrum. Next, the spectrum is filtered through bank of Mel spaced band-pass filters to obtain MFCC features.

The computed MFCC is given to GMM to generate acoustic models for healthy and disordered speech signals. GMM is state-of-the-art modeling technique [43] and have been applied in different scientific areas [44, 45]. The parameters of GMM are initialized by the k-means algorithm [46] and tuned by the well-known Expectation-Maximization algorithm [47]. Once the models are generated, then a test signal is compared with both models to determine the type of signal. If the test signal has maximum log-likelihood for the healthy model then the test signal belongs to a healthy person, otherwise, the signal belongs to a patient. To observe the effect of malicious attacks, the following measures are used for the developed disorder detection system.

Sensitivity (%): The percentage of accurately detected disordered signals from total number of disordered signals in the database.

Specificity (%): The percentage of truly detected healthy signals from total number of healthy signals in the database.

Accuracy (%): The percentage of correctly detected disordered and healthy signal from total number of signals in the database.

First, the detection system is evaluated using the original signals, then, it is evaluated for malicious attacks. The evaluation of the system with original signals is given in Table 1.

Table 1: Evaluation of disorder detection system with original signals.

Gaussian Mixtures	Specificity	Sensitivity	Accuracy
4	94.55	94.7	94.6
8	86.91	95.53	92.76
16	83.45	95.61	91.57
32	60.73	99.13	86.76
48	50.91	99.13	83.78

The good results for healthy signal is obtained with low number of mixtures and that is for disordered signals is obtained with high number of mixtures. The reason is imbalance data, i.e., the healthy signals are 53 and disordered signals are 173. The highest specificity is 94.55% and obtained with 4 mixtures. The maximum sensitivity is 99.13% and it is obtained with 48 mixtures.

To investigate the effect of malicious attacks, the signals are attacked with the noise of 20 dB and 10 dB. The evaluation of the detection system is provided in Table 2 and 3, respectively.

Table 2: Evaluation of disorder detection system with attack of 20 dB noise.

Gaussian Mixtures	Specificity	Sensitivity	Accuracy
4	82.9	94.22	91.15
8	80.2	94.80	90.71
16	78.3	95.38	90.71
32	77.1	96.53	91.15
48	75.6	97.69	91.15

Table 3: Evaluation of disorder detection system with attack of 10 dB noise.

Gaussian Mixtures	Specificity	Sensitivity	Accuracy
4	71.70	89.60	85.40
8	67.92	91.33	85.84
16	62.26	91.91	84.96
32	56.60	93.64	84.96
48	52.83	95.95	85.84

From Table 2 and 3, it can be observed that as noise increased from 20dB to 10 dB the specificity is significantly decreased. It shows that the number of false-positive increased substantially which is represents as Error in Figure 14 and 15.

In case of vocal folds disorders, vocal folds exhibit irregular vibrations. Due to this reason, disordered signals inherent some noise. Therefore, in case of noise attack, when some noise is added to healthy signals, they become similar to disordered signals. Ultimately, the detection system considered those signals as disordered signals.

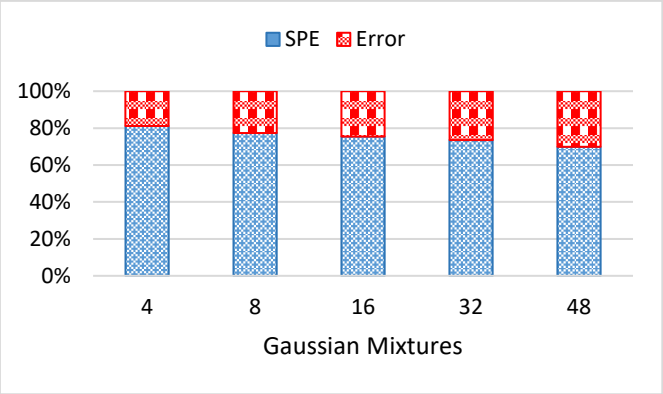


Figure 14: Specificity and false-positive rate (Error) for noise attack of 20 dB.

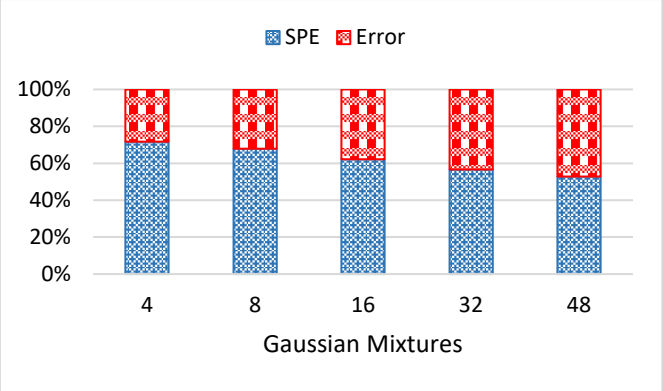


Figure 15: Specificity and false-positive rate (Error) for noise attack of 10 dB.

So, it is proved that malicious attacks greatly impact the diagnosis process. Therefore, the proposed method is designed and implemented in a way that it should capture the fabrication in the transmitted data. The proposed method is highly sensitive to the computed AMP-LBP. In case of noise attack, the characteristics of a signal changed which significantly destroy the Amp-LBP codes. Therefore, the identity will not be recovered in the original form. An identity recovered from an attacked signal is shown in Fig. 16.

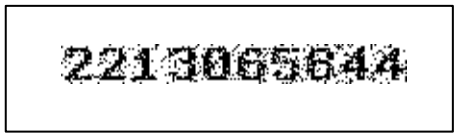


Figure 16: Identity recovered from an attacked signal of 10 dB.

Such recovered signals will indicate that the transmitted data is not in the original form and hence cannot be used for the diagnosis.

5 COMPARISON

The proposed method is compared with the existing methods to highlight the characteristics and performance of the proposed method. The comparison is provided in Table 4.

In [9], the encryption of the patient's original identity generates four secret shares. During encryption, each pixel is replaced by a 2x2 matrix which doubles each dimension of the original identity. Consequently, eight times more space required to insert these shares. In this way, for four secret shares, the space required to insert the share becomes many-folds as compared to the original identity. Sometimes, that much space is not available in a host signal to accommodate the shares. Moreover, the effect of malicious attack on accurate diagnosis of vocal folds disorder is not discussed.

In [19], the identity is directly inserted into the host signal without encryption. The identity is only protected by zero-watermarking where unauthorized access to the secret key will make the identity vulnerable. Moreover, the identity is inserted using the low-frequency regions which are robust against noise. Therefore, in case of noise attack, it cannot be determined that the identity is original or attacked. Ultimately, it will lead to false diagnosis. In [20], the identity is also directly inserted into the host signal through zero-watermarking, and the effect on disorder detection is not provided. Therefore, the authentication of the identity is impossible, which is very crucial for accurate diagnosis. The false-positive diagnosis mentally disturbs a person and resulted into loss of money and time.

The proposed method encrypts the identity of a patient into four shares, where the total dimension remains the same and no extra space is required to embed the identity into the host signal. The generated shares are embedded through zero-watermarking, and it does not affect the characteristics of the signals. In addition, the proposed method authenticates the identity of patients to avoid inevitable circumstances.

Table 4: Comparison of the characteristics of proposed method with existing methods.

Study	Encryption	Zero-watermarking	Data Authentication
[6]	✓	✓	×
[19]	×	✓	×
[20]	×	✓	×
Proposed Method	✓	✓	✓

✓ means Yes and × mean No.

6 CONCLUSIONS

A method to protect the identity of a patient is proposed in this study. The method can be used reliably in the healthcare applications due to its dual protection. The method encrypts as well as watermarked the identity using the visual cryptography and zero-watermarking without any increase in dimension of the encrypted identity. The identity of a patient cannot be revealed until unless all generated secret shares and watermark keys are available to the authorized staff members. Moreover, the proposed method does not affect the diagnosis accuracy because zero-watermarking does not change the host signal, and resultantly, the imperceptibility is naturally achieved. In addition, the proposed method also authenticates the transmitted signal based on the recovered identity. If the recovered identity is distorted, its means that the signal has been attacked and cannot be used for the diagnosis. In future, the effect of more malicious attacks on accurate diagnosis can be studied, and fragile watermarking will be implemented for integrity and authentication of the transmitted data.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia, for funding through the Research Group under Project RG-1435-051 and BTIIC (BT Ireland Innovation Centre), funded by BT and Invest Northern Ireland.

ABOUT THE AUTHORS

Zulfiqar Ali has recently joined Ulster University as a Research Fellow under the funded project of British Telecom Ireland Innovation Centre (BTIIC). He received his Ph.D. degree in 2017 from Universiti Teknologi Petronas, Malaysia, master's degree in computational mathematics from the University of the Punjab, Lahore, and another Master's degree in computer science from the University of Engineering and Technology, Lahore, with the specialization in system engineering. He was a full-time Researcher from 2010 to 2018 with the Digital Speech Processing Group, College of Computer and Information Sciences, King Saud University, Saudi Arabia. He is also a member of the Centre for Intelligent Signal and Imaging Research, Universiti Teknologi Petronas, Malaysia. His current research interests include intelligent systems, IoT frameworks, digital speech processing, medical signal processing, privacy and security in healthcare, and multimedia forensics.

Muhammad Imran is working as Assistant Professor in the College of Computer and Information Sciences, King Saud University (KSU) since 2011. He worked as a Postdoctoral Associate on joint research projects between KSU and University of Sydney, Australia. He is a Visiting Scientist with Iowa State University, USA. His research interest includes mobile ad hoc and sensor networks, WBANs, M2M, IoT, SDN, fault tolerant computing and Security and privacy. He has published number of high quality research papers in refereed international conferences and journals. His research is financially supported by several grants. Recently, European Alliance for Innovation (EAI) has appointed him as a Co-Editor in Chief for EAI Transactions on Pervasive Health and Technology. He also serves as an associate editor for IEEE Access, IEEE Communications Magazine, Wireless Communication and Mobile Computing Journal (SCIE, Wiley), Ad Hoc & Sensor Wireless Networks Journal (SCIE), IET Wireless Sensor Systems, International Journal of Autonomous and Adaptive Communication Systems (Inderscience) and International Journal of Information Technology and Electrical Engineering. He served/serving as a guest editor for IEEE Communications Magazine (SCIE), Computer Networks (SCIE, Elsevier), MDPI Sensors (SCIE), International Journal of Distributed Sensor Networks (SCIE, Hindawi), Journal of Internet Technology (SCIE), and International Journal of Autonomous and Adaptive Communications Systems. He has been involved in more than fifty conferences and workshops in various capacities such as a chair, co-chair and technical program committee member. These include IEEE ICC, Globecom, AINA, LCN, IWCMC, IFIP WWIC and BWCCA. He has received number of awards such as Asia Pacific Advanced Network fellowship.

Sally McClean (M'00) received the M.A. degree in mathematics from Oxford University, Oxford, U.K., the M.Sc. degree in mathematical statistics and operational research from Cardiff University, Cardiff, U.K., and the Ph.D. degree in mathematics (stochastic modeling) from the University of Ulster, Coleraine, U.K., in 1970, 1971, 1976, respectively. She is currently a Professor of mathematics at Ulster University. She has more than 350 publications. Her research interests include mathematical modeling, applied probability, multivariate statistical analysis, and applications to healthcare and computer science, particularly database, telecommunications and sensor technology. Dr. McClean is a Fellow of the Royal Statistical Society, the Operational Research Society, and the Institute of Mathematics and its Applications. In addition, she is the Past President of the Irish Statistical Association.

Research Group at Ulster University's Computer Science Research Institute.

Naveed Khan received his Phd degree in Computer Science from School of Computing & Information Engineering, Ulster University, UK in 2018 and M.S degree in Computer Science from King Saud University, Saudi Arabia in 2012. Currently, he is working as a Research Associate in School of Computing, Ulster University, UK. His current area of research interests includes Change detection in health sensor data, medical signal processing, Internet of Things (IoT) and Big Data Analytics.

Muhammad Shoaib received his Ph.D. degree in Communication and Information System from Beijing University of Posts and Telecommunications, China (2010). He received his M.Eng. (2005) and B.Eng. (1995) from NED University of Engineering and Technology, Karachi. His areas of research include video compression techniques, multilayer video coding, commercial Data Center facilities and IP packet based network, infrastructure and security. He worked as a Senior Manager (IP Operations, South) in Pakistan Telecommunication Company Limited, Pakistan. He also worked as a Maintenance Engineer in R. M. International. Currently, he is working as an Assistant Professor in the College of Computer and Information Sciences (Information Systems Department) in King Saud University.

REFERENCES

[1] G. K. Garge, C. Balakrishna, and S. K. Datta, "Consumer Health Care: Current Trends in Consumer Health Monitoring," *IEEE Consumer Electronics Magazine*, vol. 7, pp. 38-46, 2018.

[2] Z. Ali, G. Muhammad, and M. F. Alhamid, "An Automatic Health Monitoring System for Patients Suffering From Voice Complications in Smart Cities," *IEEE Access*, vol. 5, pp. 3900-3908, 2017.

[3] Z. Ali, M. S. Hossain, G. Muhammad, and A. K. Sangaiah, "An intelligent healthcare system for detection and classification to discriminate vocal fold disorders," *Future Generation Computer Systems*, vol. 85, pp. 19-28, 2018.

[4] H. Thapliyal, "Internet of Things-Based Consumer Electronics: Reviewing Existing Consumer Electronic Devices, Systems, and Platforms and Exploring New Research Paradigms," *IEEE Consumer Electronics Magazine*, vol. 7, pp. 66-67, 2018.

[5] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology — EUROCRYPT'94*, Berlin, Heidelberg, 1995, pp. 1-12.

[6] Z. Ali, M. Imran, M. Alsulaiman, T. Zia, and M. Shoaib, "A zero-watermarking algorithm for privacy protection in biomedical signals," *Future Generation Computer Systems*, vol. 82, pp. 290-303, 2018.

[7] Z. Ali, M. Imran, W. Abdul, and M. Shoaib, "An Innovative Algorithm for Privacy Protection in a Voice Disorder Detection System," Cham, 2018, pp. 228-233.

[8] W. Abdul, Z. Ali, S. Ghouzali, and M. Alsulaiman, "Security and Privacy for Medical Images Using Chaotic Visual Cryptography," *Journal of Medical Imaging and Health Informatics*, vol. 7, pp. 1296-1301, 2017.

[9] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, and M. S. Hossain, "Biometric Security Through Visual Encryption for Fog Edge Computing," *IEEE Access*, vol. 5, pp. 5531-5538, 2017.

[10] R. Eswaraiah and E. S. Reddy, "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest," *IET Image Processing*, vol. 9, pp. 615-625, 2015.

[11] A. Singh, M. K. Dutta, J. Prinosil, and K. Riha, "Wavelet based robust watermarking scheme for copyright enforcement and integrity control in tele-ophthalmology," in *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2016, pp. 408-413.

[12] M. Alhussein and G. Muhammad, "Watermarking of Parkinson Disease Speech in Cloud-Based Healthcare Framework," *International Journal of Distributed Sensor Networks*, vol. 11, p. 264575, 2015.

[13] M. K. Dutta, A. Singh, A. Singh, R. Burget, and J. Prinosil, "Digital identification tags for medical fundus images for tele-ophthalmology applications," in *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, 2015, pp. 781-784.

[14] E. Walia and A. Suneja, "Fragile and blind watermarking technique based on Weber's law for medical image authentication," *IET Computer Vision*, vol. 7, pp. 9-19, 2013.

[15] Z. Pakdaman, S. Saryazdi, and H. Nezamabadi-pour, "A prediction based reversible image watermarking in Hadamard domain," *Multimedia Tools and Applications*, vol. 76, pp. 8517-8545, March 01 2017.

[16] S. Abhilasha and D. Malay Kishore, "A Reversible Data Hiding Scheme for Efficient Management of Tele-Ophthalmological Data," *International Journal of E-Health and Medical Communications (IJEHMC)*, vol. 8, pp. 38-54, 2017.

[17] L. Zhang, P. Cai, X. Tian, and S. Xia, "A novel zero-watermarking algorithm based on DWT and edge detection,"

in *2011 4th International Congress on Image and Signal Processing*, 2011, pp. 1016-1020.

[18] J. Zhao, W. Xu, S. Zhang, S. Fan, and W. Zhang, "A Strong Robust Zero-Watermarking Scheme Based on Shearlets' High Ability for Capturing Directional Features," *Mathematical Problems in Engineering*, vol. 2016, p. 11, 2016.

[19] Z. Ali, M. Imran, M. Alsulaiman, M. Shoaib, and S. Ullah, "Chaos-based robust method of zero-watermarking for medical signals," *Future Generation Computer Systems*, vol. 88, pp. 400-412, 2018.

[20] Z. Ali, M. S. Hossain, G. Muhammad, and M. Aslam, "New Zero-Watermarking Algorithm Using Hurst Exponent for Protection of Privacy in Telemedicine," *IEEE Access*, vol. 6, pp. 7930-7940, 2018.

[21] A. Al-Nasheri, G. Muhammad, M. Alsulaiman, Z. Ali, K. H. Malki, T. A. Mesallam, *et al.*, "Voice Pathology Detection and Classification Using Auto-Correlation and Entropy Features in Different Frequency Regions," *IEEE Access*, vol. 6, pp. 6961-6974, 2018.

[22] G. Muhammad, G. Altuwaijri, M. Alsulaiman, Z. Ali, T. A. Mesallam, M. Farahat, *et al.*, "Automatic voice pathology detection and classification using vocal tract area irregularity," *Biocybernetics and Biomedical Engineering*, vol. 36, pp. 309-317, 2016.

[23] Z. Ali, M. Alsulaiman, I. Elamvazuthi, G. Muhammad, T. A. Mesallam, M. Farahat, *et al.*, "Voice pathology detection based on the modified voice contour and SVM," *Biologically Inspired Cognitive Architectures*, vol. 15, pp. 10-18, 2016.

[24] M. Alhussein, Z. Ali, M. Imran, and W. Abdul, "Automatic Gender Detection Based on Characteristics of Vocal Folds for Mobile Healthcare System," *Mobile Information Systems*, vol. 2016, p. 12, 2016.

[25] R. Jardim, S. M. Barreto, and A. Á. Assunção, "Voice Disorder: case definition and prevalence in teachers," *Revista Brasileira de Epidemiologia*, vol. 10, pp. 625-636, 2007.

[26] A. Al-nasheri, Z. Ali, G. Muhammad, and M. Alsulaiman, "Voice pathology detection using auto-correlation of different filters bank," in *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, 2014, pp. 50-55.

[27] J. Bohlender, "Diagnostic and therapeutic pitfalls in benign vocal fold diseases," *GMS Curr Top Otorhinolaryngol Head Neck Surg*, vol. 12, p. Doc01, 2013.

[28] T. A. Mesallam, M. Farahat, K. H. Malki, M. Alsulaiman, Z. Ali, A. Al-nasheri, *et al.*, "Development of the Arabic Voice Pathology Database and Its Evaluation by Using Speech Features and Machine Learning Algorithms," *Journal of Healthcare Engineering*, vol. 2017, p. 13, 2017.

[29] L. H. Rosenthal, M. S. Benninger, and R. H. Deeb, "Vocal fold immobility: a longitudinal analysis of etiology over 20 years," *Laryngoscope*, vol. 117, pp. 1864-70, Oct 2007.

[30] T. Mau, "Diagnostic evaluation and management of hoarseness," *Med Clin North Am*, vol. 94, pp. 945-60, 2010.

[31] K. Simonyan, F. Tovar-Moll, J. Ostuni, M. Hallett, V. F. Kalasinsky, M. R. Lewin-Smith, *et al.*, "Focal white matter changes in spasmodic dysphonia: a combined diffusion tensor imaging and neuropathological study," *Brain*, vol. 131, pp. 447-59, 2008.

[32] Massachusette Eye & Ear Infirmry Voice & Speech LAB, "Disordered Voice Database Model 4337 (Ver. 1.03) ", ed. Boston, MA: Kay Elemetrics Corp, , 1994.

[33] Z. Ali, M. Talha, and M. Alsulaiman, "A Practical Approach: Design and Implementation of a Healthcare Software for Screening of Dysphonic Patients," *IEEE Access*, vol. 5, pp. 5844-5857, 2017.

[34] Z. Ali, M. Alsulaiman, G. Muhammad, I. Elamvazuthi, A. Al-nasheri, T. A. Mesallam, *et al.*, "Intra- and Inter-database Study for Arabic, English, and German Databases: Do Conventional Speech Features Detect Voice Pathology?," *Journal of Voice*, vol. 31, pp. 386.e1-386.e8, 2017.

[35] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Generation Computer Systems*, vol. 85, pp. 76-87, 2018.

[36] Z. Ali, I. Elamvazuthi, M. Alsulaiman, and G. Muhammad, "Automatic Voice Pathology Detection With Running Speech by Using Estimation of Auditory Spectrum and Cepstral Coefficients Based on the All-Pole Model," *Journal of Voice*, vol. 30, pp. 757.e7-757.e19, 2016.

[37] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612-613, 1979.

[38] H. E. Hurst, "Long-term storage of reservoirs: an experimental study," *Transactions of the American Society of Civil Engineers* vol. 116, pp. 770-799, 1951.

[39] M. R. L. Hodges, "Effect of threshold offsets in zero-crossing speech detector," *Electronics Letters*, vol. 17, pp. 682-684, 1981.

[40] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 24, pp. 971-987, 2002.

[41] A. Zulfiqar, A. Muhammad, A. M. Martinez-Enriquez, and G. Escalada-Imaz, "Text-Independent Speaker Identification Using VQ-HMM Model Based Multiple Classifier System," Berlin, Heidelberg, 2010, pp. 116-125.

[42] M. Alsulaiman, G. Muhammad, and Z. Ali, "Comparison of voice features for Arabic speech recognition," in *2011 Sixth International Conference on Digital Information Management*, 2011, pp. 90-95.

[43] C. M. Bishop, *Pattern Recognition and Machine Learning*: Springer-Verlag New York, 2006.

[44] Z. Ali, M. Imran, and M. Alsulaiman, "An Automatic Digital Audio Authentication/Forensics System," *IEEE Access*, vol. 5, pp. 2994-3007, 2017.

[45] Z. Ali, M. Alsulaiman, G. Muhammad, A. Al-nasheri, and A. Mahmood, "Clinical informatics: mining of pathological data by acoustic analysis," in *2017 International Conference on Informatics, Health & Technology (ICIHT)*, 2017, pp. 1-8.

[46] T. Kanungo, D. M. Mount, N. S. Netanyahu, C. D. Piatko, R. Silverman, and A. Y. Wu, "An efficient k-means clustering algorithm: analysis and implementation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 881-892, 2002.

[47] R. A. Redner and H. F. Walker, "Mixture Densities, Maximum Likelihood and the EM Algorithm," *SIAM Review*, vol. 26, pp. 195-239, 1984.